ActiveSync Distributed Agency Testing

This document is intended to provide a step by step process for State agencies to follow if they want a new mobile device added to the CTS ActiveSync Approved Device list. Also contained is an ActiveSync device test matrix.

Step by step process *Note: Commonly used PowerShell commands for managing ActiveSync users are included*.

Customer Agency Support Staff

1. Receives request from an individual or agency request to add new mobile device to the CTS ActiveSync Approved Device list.
2. Request for new device is forwarded to agency Help Desk.
3. Determine if requested device already exists on CTS approved device list or new device? If it is already on the list, then no further action is required, simply activate the device using the user's Active Directory credentials [OWA logon info], network/Active Directory password, and the name of the Exchange server: mobile.wa.gov
4. Prepare agency ActiveSync test email box for new device testing by first enabling the mailbox for ActiveSync – PowerShell command:
   Set-CASMailbox "full email address" -ActiveSyncEnabled $true
5. Assign appropriate ActiveSync policy to the agency test mail box based on type of device. Please see ActiveSync Device Policy matrix: http://cts.wa.gov/projects/shared_email/docs/ActiveSync_DRAFT_Device_List_by_Policy.doc Note: Policy1 is typically Apple products, & Policy2 Android products, Policy3 for some Android and Windows 7.5/8– PowerShell command:
   Set-CASMailbox "full email address"-ActiveSyncMailboxPolicy Policy1
6. Ensure no ActiveSync device models/IDs are associated with the agency test email box – clear &/or delete using PowerShell or from test account OWA menu options.
   a. Obtain the Identity to delete– PowerShell command
      Get-ActiveSyncDeviceStatistics -Mailbox john.doe@cts.wa.gov | fl Identity
   b. Clear/wipe remotely– PowerShell command:
      Clear-ActiveSyncDevice -identity "dis.wa.lcl/CTS/Users/UserAccounts/Doe, John (CTS)/ExchangeActiveSyncDevices/SAMSUNGSGHT999§SEC1325376100442"
   c. Delete ActiveSync Device IDs- PowerShell command:
      Set-CASMailbox "alias" -ActiveSyncAllowedDeviceIDs: $nul
7. Activate device using agency EAS test mail box.
8. Ensure the policy has been applied to the mailbox – AppliedInFull. If the policy is not 'AppliedInFull', then try another ActiveSync policy – see policy set command above– PowerShell command:
   Get-ActiveSyncDeviceStatistics -mailbox "full email address" | fl identity,device*,last*

NOTE: If none of the policies can be 'AppliedInFull', then the device fails at the activation stage because policies that meet OCIO requirements cannot successfully be pushed to that device, no further testing is required.

9. Agency ActiveSync test mail box receives an ActiveSync Quarantine message as does the CTS Mobile Messaging group.
10. If AppliedInFull in the appropriate policy, then contact CTS Service Desk and open a ticket and have it assigned to the CTS Mobile Messaging group to release agency EAS test mailbox from ActiveSync quarantine. Please provide the CTS Service Desk with a copy of the quarantine message so that they can attach that to the ticket, along with the results of this PowerShell command:

    Get-ActiveSyncDeviceStatistics -mailbox john.doe@cts.wa.gov | fl

    NOTE: If an agency discovers during testing that the policy that the agency EAS test mailbox is assigned to allows functionality on that device that is too permissive and does not meet or exceed OCIO requirements, then that device must be failed in that policy. If device fails in all policies [too permissive], then the device must fail, and those results recorded & reported to CTS so can be posted on the CTS ActiveSync web site for all agencies to view.

CTS Service Desk

11. Receives customer request, creates ticket and assigns to the CTS Mobile Messaging group. Please attach or include the PowerShell command results provided by the customer agency, a completed test matrix & CIO approval when appropriate.

CTS Mobile Messaging

12. Receives ticket from CTS Service Desk to release account/mail box from ActiveSync quarantine. Verify IT policy is AppliedInFull, then release device/user from quarantine – Allow only the 'individual' in Exchange, then contact customer agency support staff and let them know they can proceed with testing.

Customer Agency Support Staff

13. Test device using the CTS ActiveSync device test matrix. Please see test matrix below. Test categories:
    a. Device lock password.
    b. Verify email flow and calendar sync on device.
    c. Device locks after 60 minutes or less of non-use.
    d. Device wipes after 10 bad passwords have been entered.
    e. Remote wipe of device from OWA.
    f. Encryption of the device.
14. If device Fails to meet OCIO requirements in all ActiveSync policies, then email the completed test matrix to the CTS Mobile Messaging group.
15. If device Passes OCIO requirements in all ActiveSync policies, then email the completed test matrix to the agency CIO for their final approval.
16. Agency CIO: Approve device testing meets or exceeds OCIO requirements and emails the completed test matrix to the CTS Mobile Messaging group along with approval.

CTS Mobile Messaging

17. Record results and forward to service owner for review and approval.
18. Add new customer agency tested device to the CTS ActiveSync Approved Device list & create a new Allow rule for that device in Exchange so that specific 'device model' will now bypass quarantine on all future activations for any agency using the specific 'device model'.
19. Coordinate posting results on CTS ActiveSync web site of newly approved devices with internal web design group, communicate status to requesting customer agency, and close the CTS ticket.

ActiveSync Device Test Matrix

Date Tested:	
Person Testing & Agency:	
Device: State Owned / BYOD:	
Carrier:	
Manufacturer:	
Device Model:	
OS Version:	
ActiveSync Policy Used to Approve Device:	

Complete this box after testing

Pass / Fail

Test Case#		Test Case Description	Test Results
1	☐	Assign your test mailbox to an ActiveSync Policy based on manufacturer & model to start with:	
		http://cts.wa.gov/projects/shared_email/docs/ActiveSync_DRAFT_Device_List_by_Policy.doc	
		Give the policy time to replicate between the CAS servers.	
2	☐	Attempt to sync with ActiveSync and receive a quarantine e-mail message	
		Reported Device Model in Quarantine message:	
3	☐	Ensure the policy has been applied to the account	PASS / FAIL
		If policy is not "AppliedInFull", then try another policy.	
		Get-ActiveSyncDeviceStatistics -mailbox john.doe@cts.wa.gov | fl identity,device*,last*	
		`DevicePolicyApplicationStatus : AppliedInFull`	
		NOTE: If none of the policies can be 'AppliedInFull', then the device fails at the activation stage because policies that meet OCIO requirements cannot successfully be pushed to that device, no further testing is required.	
		Reported Device Model returned by above PowerShell:	
4	☐	Contact CTS Service and open a ticket and have it assigned to the CTS Mobile Messaging group.	
		State in the request, you would like the attached Device ID/model allowed for your agency's	
		ActiveSync test account, please include the name of the account used.	
5	☐	Receive communication from CTS Mobile Messaging stating that the device has been allowed for	
		your account.	
6	☐	Accept the policy settings that are pushed to the device and the final step will be to enter valid	
		device lock/unlock password.	

7	☐	Test Passwords for the device lock screen:	PASS / FAIL
		Password [ ] Should fail	
		1Password [ ] May fail (If this passes then most likely the device distinguishes upper and lower case)	
		@Password [ ] May fail (If this passes then most likely the device distinguishes upper and lower case)	
		###### [ ] Should fail	
		123456 [ ] Should fail	
		q!@#1 [ ] Should fail	
		@1Pass [ ] Should Pass	
		qa2!@# [ ] Should Pass	
		Select a password that meets or exceeds OCIO requirements & continue to next test.	
		NOTE: If the device cannot pass this testing phase, then testing is completed. The device does not meet OCIO requirements.	
8	☐	Continue setting up the ActiveSync device & verify e-mail is syncing on the device:	
		http://cts.wa.gov/projects/shared_email/docs/ActiveSync_End_User_Guide.doc	
9	☐	Lock the device and enter 10 bad passwords at the unlock screen. The device should execute a	PASS / FAIL
		If the device wipes successfully, then pass and go to the next test, else fail.	
		NOTE: If the device cannot pass this testing phase, then testing is completed. The device does not meet OCIO requirements.	
10	☐	After 60 minutes or less of inactivity on the device it requires you to enter the unlock passwor	PASS / FAIL
		If the device locks successfully after 60 minutes or less or inactivity, then pass and go to the next test, else fail.	
		NOTE: If the device cannot pass this testing phase, then testing is completed. The device does not meet OCIO requirements.	
11	☐	Remote wipe the device from OWA	PASS / FAIL
		In OWA: Options / See All Options... / Phone : Select the phone and choose 'Wipe Device'	
		Device wipes: Confirm that the device is factory reset	
		After the device wipes there should be a confirmation e-mail confirming the remote device wipe.	
		In OWA: Remove the phone from the Account to prevent it from wiping again.	
		NOTE: If the device cannot pass this testing phase, then testing is completed. The device does not meet OCIO requirements.	

12	☐	Test Encryption - not an OCIO requirement:	PASS / FAIL
		Move the device to the same policy number w/ encryption. i.e. Policy2-Encryption	
		Give the policy change time to replicate between the CAS servers	
		The device will display a new message regarding Data Encryption Policy	
		Click OK to start the encryption process	
		After the encryption process completes send a test e-mail from the device	
13		**Informational Tests**	
	☐	Change Password on AD account and note how device handles this	
		Notes:	
	☐	One month of data shows on calendar	
		Notes:	
	☐	One month of data shows in e-mail	
		Notes:	
	☐	User must change password every 120 days	
		Notes:	
	☐	Apple devices: No Recovery Password option is available in OWA.	
	☐	Device requests recovery password: Obtain Revcovery Password From OWA and enter it on the device.	
		Device accepts recovery password? If yes perform next step. If not then contact CTS Mobile Messaging. Verify it won't accept the old password as new password: True = Pass	